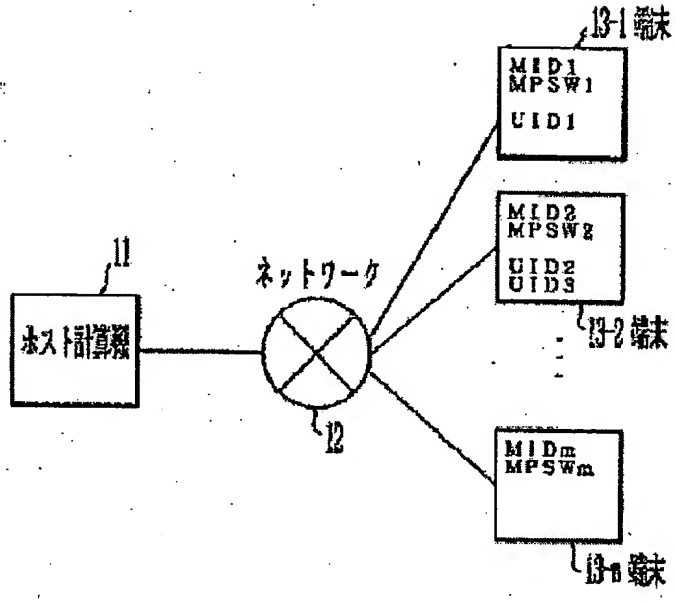
Publication number: JP2001357156
Publication date: 2001-12-26
Inventor: OKADA TOSHIO; IGARASHI NORIHIKO; OKI HIROSHI; KAMATA SHINJI; HARA TAKASHI; YAMAZAKI TOSHIYA
Applicant: FUJITSU LTD
Classification:
- international: *G06Q50/00; G06F1/00; G06F21/22; G06Q30/00;* G06Q50/00; G06F1/00; G06F21/22; G06Q30/00; (IPC1-7): G06F17/60; G06F1/00
- european:
Application number: JP20010124997 20010423
Priority number(s): JP20010124997 20010423

Abstract of **JP2001357156**

PROBLEM TO BE SOLVED: To monitor illegal copying by managing a distribution destination of distributed software with information including an identifier. SOLUTION: When a host computer 11 at a distribution center sells software through a network 12 at a request from a user terminal, each terminal is given a terminal identifier (MID) and a terminal password (MPSW) and the user is given a user identifier(UID) and a user password. The software is sold having a distribution identifier embedded. The host computer 11 relates those identifier to password and manages a history of sale. When the sold software is destroyed, restoration service is provided by referring the sale history. Each time the host computer 11 is accessed, the terminal password of the terminal is rewritten and it is checked whether or not the host computer is accessed by using the latest terminal password.

実施例の構成図



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－357156
（P2001－357156A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	１４２	Ｇ０６Ｆ　17/60	１４２	５Ｂ０７６
	３０２		３０２Ｅ	
	３３２		３３２	
1/00		9/06	６６０Ｃ	

審査請求　有　　請求項の数２　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－124997(P2001－124997)
(62)分割の表示　特願平7－1798の分割
(22)出願日　平成７年１月10日(1995.1.10)

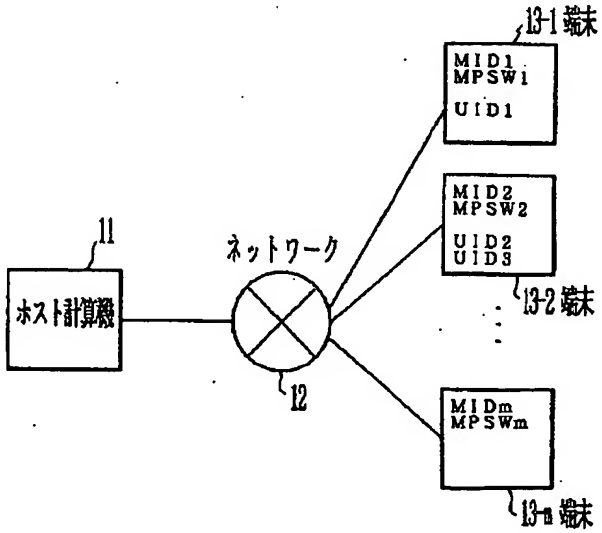
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　岡田　利司郎
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　五十嵐　典彦
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　100074099
弁理士　大菅　義之　（外１名）

最終頁に続く

(54)【発明の名称】　ソフトウェア流通システムにおける識別子管理装置及び方法

(57)【要約】
【課題】流通ソフトウェアの配布先を識別子を含む情報によって管理し、不正コピーを監視する。
【解決手段】流通センターのホスト計算機１１がユーザの端末からの要請に応じて、ネットワーク１２を介してソフトウェアを販売する際、各端末には、それぞれの端末識別子（ＭＩＤ）及び端末パスワード（ＭＰＳＷ）が付与され、ユーザには、ユーザ識別子（ＵＩＤ）及びユーザパスワードが付与される。また、ソフトウェアには、ディストリビューション識別子が埋め込まれて販売される。ホスト計算機１１は、これらの識別子及びパスワードを関連付けて、販売の履歴を管理する。販売したソフトウェアが破壊されたときは、その販売記録を参照して復旧サービスが行われる。また、ホスト計算機１１にアクセスするたびに、端末の端末パスワードは書き換えられ、最新の端末パスワードを用いてアクセスしているかどうかがチェックされる。

実施例の構成図



1

【特許請求の範囲】

【請求項１】　端末に関する情報に関連付けてソフトウェアの配布記録を行う手段と、
ユーザに関する情報と端末に関する情報を関連付けて記憶する記憶手段と、
前記配布記録と前記記憶手段に記憶された情報に基づいて、該当するユーザに課金する手段とを有するソフトウェア流通管理装置。

【請求項２】　端末に関する情報に関連付けてソフトウェアの配布記録するステップと、
ユーザに関する情報と端末に関する情報を関連付けた記憶情報と前記配布記録に基づいて、該当するユーザに課金するステップを有するソフトウェア流通方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークを介したソフトウェアの流通（ディストリビューション）システムに係り、ソフトウェアの配布先の識別子を管理する装置とその方法に関する。

【０００２】

【従来の技術】現在、店頭で販売されているパッケージソフトウェアは、一般に、インストールするパソコン等のマシンの台数や同時に動作可能なマシンの台数に制限を設けていることが多い。例えば、１台のパソコンのみにインストール可能であるとか、または複数のパソコンにインストール可能だが、そのうち同時に動作してもよい台数は１台のみであるというような制限である。

【０００３】例えば、ＷＩＮＤＯＷＳ（登録商標）上に搭載されるソフトウェア等においてはその不正コピーを抑制するため、インストール時にライセンス登録情報をフロッピー（登録商標）ディスク上のソフトウェアに書き込むことが一般的になってきている。しかし、このライセンス登録情報はときとして偽りの情報であったり、フリーウェア等で後から自由に書き直したりすることが可能であったりするため、十分な効果が得られていない。

【０００４】一方、近年のパソコン通信等の発達に伴い、ネットワークを介してオンラインでソフトウェアを購入できることが望まれている。このようなソフトウェアの流通を実現するにあたって、ベンダーとユーザの間におけるソフトウェアの使用契約等のいくつかの問題がある。例えば、上述したようなソフトウェアのインストール時および使用時における制限を設け、それを実施するためには、ソフトウェアの使用状況を管理する工夫が必要になる。

【０００５】

【発明が解決しようとする課題】ネットワークを介したオンラインのソフトウェア流通システムを構築するには次のような問題がある。フロッピーディスクを利用した現在のプロテクション方法は用いることができず、インストールしたマシンから別のマシンへソフトウェアが不正にコピーされる恐れがあり、このような不正コピーを監視する機構が必要になる。

2

【０００６】また、何らかの原因によりインストールしたソフトウェアが破壊されて使用不可能となったときに、ユーザの復旧要請に応じる必要がある。また、将来、オンラインによるソフトウェアの流通が一般に普及した場合に、配布したソフトウェアを個別に識別する機構が必要になる。

【０００７】本発明は、ネットワークを介したソフトウェアの流通システムにおいて、ソフトウェアの配布先の識別子を含む情報を管理し、ベンダーまたはユーザの利益を図る識別子管理装置とその方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、流通センターとユーザの端末とをネットワークで結び、流通センターからオンラインでソフトウェアを端末に配布するソフトウェア流通システムにおける識別子管理装置および識別子管理方法である。

【０００９】図１は、本発明の識別子管理装置の原理図である。図１の識別子管理装置は、管理手段１、端末パスワード変更手段２、ディストリビューション識別子付加手段３、ユーザ情報記憶手段４、端末情報記憶手段５、配布記録記憶手段６、定義ファイル格納手段７、およびソフトウェア格納手段８を備える。

【００１０】ソフトウェア格納手段８は配布するソフトウェアを格納し、ユーザ情報記憶手段４はソフトウェアの配布先のユーザの識別子を含むユーザ情報を記憶し、端末情報記憶手段５はソフトウェアがインストールされる端末の識別子を含む端末情報を記憶する。管理手段１は、ユーザ情報記憶手段４に記憶された上記ユーザ情報と端末情報記憶手段５に記憶された上記端末情報とを関連付けて管理する。

【００１１】配布記録記憶手段６はソフトウェアの配布記録を上記端末の識別子と関連付けて記憶し、管理手段１は前記ユーザ情報と上記端末情報と上記配布記録とを用いて、ソフトウェアの配布の履歴を管理する。また、端末情報記憶手段５は上記端末の識別子に対応して付与された第１の端末パスワードを含む上記端末情報を記憶し、管理手段１は上記端末の識別子と上記第１の端末パスワードとを用いて端末からのアクセスを識別する。

【００１２】端末パスワード変更手段２は上記第１の端末パスワードを持つ端末からのアクセスがあったとき、第１の端末パスワードを第２の端末パスワードに変更し、管理手段１は第２の端末パスワードを上記端末の識別子に対応させる。定義ファイル格納手段７はディストリビューション識別子の書き込みのための情報を記述した定義ファイルを格納する。ソフトウェアを配布するときに、ディストリビューション識別子付加手段３は定義

ファイル格納手段７に格納された上記定義ファイルを参照して、ソフトウェア格納手段８に格納されたソフトウェア内に上記ディストリビューション識別子を書き込むとともに、配布記録記憶手段６に記憶された上記配布記録に上記ディストリビューション識別子を書き込む。

【００１３】また、管理手段１は上記定義ファイルを参照して、上記流通センターにアクセスするユーザが持っているソフトウェアの上記ディストリビューション識別子をチェックする。図１の管理手段１、端末パスワード変更手段２、およびディストリビューション識別子付加手段３は、図２に示す実施例におけるホスト計算機１１内の図示されない処理装置に相当する。また、図１のユーザ情報記憶手段４、端末情報記憶手段５、配布記録記憶手段６、定義ファイル格納手段７、およびソフトウェア格納手段８は、図２のホスト計算機１１内の図示されない記憶装置に相当する。

【００１４】また、上記配布記録は例えば図４、５、および１３に示す販売記録に相当し、上記定義ファイルに記述された上記書き込みのための情報とは、例えば上記ディストリビューション識別子を書き込むファイルの名称、そのファイル内の書き込み領域の位置、その書き込み領域の大きさ等の情報である。

【００１５】管理手段１によりユーザ情報記憶手段４の記憶するユーザの識別子と端末情報記憶手段５の記憶する端末の識別子とが関連付けて管理される。これにより、ソフトウェアがどのユーザに対して配布され、またその際どの端末にインストールされたかが同時に把握される。

【００１６】さらに、配布記録記憶手段６が記憶する配布記録が上記端末の識別子と関連付けられるので、一つ一つのソフトウェアの配布の履歴がインストールした端末の端末情報とともに管理される。また、端末情報記憶手段５内の端末情報と端末内の双方に、上記端末の識別子に対応した第１の端末パスワードが保持される。端末からのアクセスがあったとき、管理手段１は上記端末の識別子と第１の端末パスワードとを用いて、アクセスした端末を識別する。例えば、アクセスした端末の持つ端末パスワードがその端末の識別子に対応していない場合は、その端末側に何らかの異変があったとみなすことができる。

【００１７】さらに、端末からのアクセスがあったとき、端末パスワード変更手段２によりその端末の第１の端末パスワードが第２の端末パスワードに変更される。これにより、次回のアクセス時には、上記端末の識別子と第２の端末パスワードとを用いて端末の識別が行われる。もし、ユーザが端末にインストールされたソフトウェアを上記端末の識別子と第１の端末パスワードとともに別の端末にコピーして、次回のアクセス時に別の端末からアクセスしても、既に第１の端末パスワードは有効性を失っているため管理手段１は異変を察知することができる。

【００１８】また、定義ファイル格納手段７内の定義ファイルに記述された書き込みのための情報に従って、ディストリビューション識別子付加手段３により、配布するソフトウェア内にディストリビューション識別子が書き込まれる。管理手段１は上記定義ファイルを参照して、ユーザの持つソフトウェアの上記ディストリビューション識別子をチェックすることができる。例えば、上記ディストリビューション識別子として配布先のユーザの識別子を用いれば、アクセスしてきたユーザが配布時のユーザと同一かどうかがわかる。

【００１９】配布記録記憶手段６内の上記配布記録にも上記ディストリビューション識別子を書き込んでおくことにより、管理手段１は上記配布記録内のディストリビューション識別子とユーザの持つソフトウェア内に書き込まれたものとを比較できる。

【００２０】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施例について詳細に説明する。図２は、本発明の一実施例のソフトウェア流通システムの構成図である。図２のソフトウェア流通システムは、ホスト計算機１１と複数（ｍ個）のユーザ端末１３－１、・・・、１３－ｍ、およびそれらを結合するネットワーク１２から成る。

【００２１】ホスト計算機１１はソフトウェアの流通センターにあり、端末１３－１、・・・、１３－ｍからの要請に応じて、ネットワーク１２を介してソフトウェアを販売する。端末１３－１、・・・、１３－ｍは例えばユーザの自宅やオフィス等に設置されたパソコン等の計算機であり、ネットワーク１２を介して希望するソフトウェアを購入し、購入したソフトウェアを使用してホスト計算機１１にアクセスする。

【００２２】ホスト計算機１１は本発明の識別子管理装置を含み、販売するソフトウェアを格納するための図示されない記憶装置を有する。ホスト計算機１１は端末１３－１、・・・、１３－ｍにそれぞれの端末識別子（マシンＩＤ）ＭＩＤ１、・・・、ＭＩＤｍを発行し、端末のユーザにはマシンＩＤとは別のユーザ識別子（ユーザＩＤ）ＵＩＤ１、ＵＩＤ２、ＵＩＤ３等を発行する。また、各マシンＩＤに対応して端末のパスワード（マシンパスワード）ＭＰＳＷ１、・・・、ＭＰＳＷｍを設け、各ユーザＩＤに対応してユーザパスワード（不図示）を設ける。ホスト計算機１１はこれらのマシンＩＤ、マシンパスワード、ユーザＩＤ、およびユーザパスワードを用いて、ソフトウェアの販売先である端末とユーザの情報を管理する。

【００２３】ユーザに販売したソフトウェアが何らかの原因により破壊され使用不可能となった場合には、ホスト計算機１１は販売記録を参照して、そのソフトウェアの復旧サービスを行う。また、販売したソフトウェアの

バージョンアップのサービスも行う。さらに、ホスト計算機１１は端末に与えるマシンパスワードを動的に変更して、アクセスが行われるたびにそれをチェックすることにより、インストールしたソフトウェアが他の端末にコピーされたかどうかを監視する。

【００２４】あるユーザから他のユーザに端末の譲渡があった場合には、その端末にインストールされたソフトウェアは、そのバージョンアップや復旧等のサービスを受ける権利も含めて譲り渡すことが可能となる。このような譲渡を行えば、不正コピーの防止にも繋がるし、権利の譲渡もスムーズに行われるため、ユーザとベンダーの双方に有益に働く。

【００２５】図３および図４は、それぞれホスト計算機１１内の記憶領域に格納されるユーザ情報および端末情報（マシン情報）の例を示している。図３のユーザ情報は、ユーザＩＤ（ＵＩＤ）、ユーザパスワード（ＰＳＷ）、マシンＩＤ（ＭＩＤ）、ユーザの名前等から成り、図４のマシン情報は、ＭＩＤ、マシンパスワード（ＭＰＳＷ）、ＵＩＤ、端末の機種、ソフトウェアの販売記録等から成る。

【００２６】図５は、図４のソフトウェアの販売記録の例を示している。図５の販売記録は、販売したソフトウェアの名称（ソフトウェア名）、購入したユーザのＵＩＤ、販売日時から成る。このように、ホスト計算機１１はＭＩＤ、ＵＩＤ、およびソフトウェアの販売記録を互いに関連付けて記憶し、ソフトウェアの販売先の情報として管理する。これにより、いつ、誰が、どの端末に、どんなソフトウェアをインストールしたかを示す販売履歴の管理が可能となる。また、そのソフトウェアに関するバージョンアップ等のサービス情報を購入したユーザのみに選択的に提供して、購入者を優遇することもできる。

【００２７】ところで、個人や企業がパソコン等の端末を持つ場合、ソフトウェアの購入のために代金を支払う人と購入したソフトウェアを使用する人の関係、あるいはソフトウェアを購入または使用する人と端末との関係が必ずしも１対１の関係では無く、次のような形態が生じ得る。

（１）１人のユーザが複数台の端末を持つ。

（２）複数のユーザが１台の端末を共有する。

（３）（１）と（２）の混合形態。

【００２８】これらの各形態に対応するソフトウェアの使用契約としては、次のような形態が考えられる。

（１）１台の端末にのみソフトウェアのインストールが許される。

（２）複数の端末にソフトウェアをインストールしてもよいが、そのソフトウェアを２つ以上の端末上で同時に使用することは禁止される。

（３）複数の端末にソフトウェアをインストールして、それらの端末上で同時に使用してもよい（フリーウェア）。

【００２９】また、これらの各契約形態に対応する管理方法は次のようになる。

（１）ソフトウェアをどの端末にインストールしたかを、ＭＩＤと関連させて管理する必要がある。

（２）ソフトウェアをどのユーザに販売したかを、ＵＩＤと関連させて管理する必要がある。

（３）フリーウェア等に相当し、販売先の管理は不要である。

【００３０】上記（１）および（２）の使用形態を管理するには、ＭＩＤとＵＩＤの両方を用いる必要がある。本実施例では、流通センターのホスト計算機１１が契約したすべてのユーザにユニークなＵＩＤを与え、また契約したすべての端末にユニークなＭＩＤを与える。

【００３１】ホスト計算機１１は商品（ソフトウェア）の販売時に、ＵＩＤを用いて代金を支払うべきユーザを特定する。したがって、あるＵＩＤを用いて販売されたソフトウェアの代金は、そのＵＩＤを持つユーザが支払う契約になっている。また、販売された商品はその販売先の端末のＭＩＤと関連付けられて管理される。これにより、ある商品を誰が購入し、どの端末にインストールされたかが明確になり、その商品が破壊された場合でも無償の復旧サービス等を提供することが可能になる。

【００３２】図６は、１人のユーザが複数の端末を持つ場合に、ホスト計算機１１が管理する情報の関係を示している。図６において、ユーザ情報は、ＵＩＤ＝０１、ユーザの氏名、キャッシュカードの情報（キャッシュカードの番号等）、およびソフトウェアの購入情報から成る。購入情報は過去にそのユーザが流通センターから購入したソフトウェア名と購入金額のリストであり、例えばそのユーザのＵＩＤを持つ販売記録を参照して得ることができる。ここでは、ＵＩＤ＝０１を持つユーザがＬＯＴＵＳ－ＷＩＮ、ＦＭ秘書、ＬＯＴＵＳ、ＯＡＳＹＳの各ソフトウェアを購入したことがわかる。

【００３３】ＵＩＤ＝０１のユーザが持つ３つの端末ＰＣ９８、ＴＯＷＮＳ、およびＦＭＲのうち、ＭＩＤ＝１１のＰＣ９８とＭＩＤ＝１０のＴＯＷＮＳとがホスト計算機１１に登録されており、その登録時にＵＩＤ＝０１と関係付けられる。登録時には、図４に示すように端末のマシン情報にＵＩＤを書き込んでもよく、あるいはまた、ポインタ等を用いてマシン情報とユーザ情報を結びつけてもよい。

【００３４】登録された端末のマシン情報は、ＭＩＤ、過去に販売されてその端末にインストールされたソフトウェアの情報（ソフト情報）、および端末の機種や使用ＯＳ（オペレーティングシステム）の情報から成る。ソフト情報は図４の販売記録に相当する。ここでは、ＭＩＤ＝１１の端末にインストールされたソフトウェアがＬＯＴＵＳであり、その機種（Ｍ）は９８、使用ＯＳはＤＯＳであることがわかる。また、ＭＩＤ＝１０の端末に

インストールされたソフトウェアはＬＯＴＵＳ－ＷＩＮであり、その機種はＴＯＷＮＳ、使用ＯＳはＤＯＳ、ＴＯＳ（ＴＯＷＮＳ用のＯＳ）、およびＷＩＮ（ＷＩＮＤＯＷＳ）であることがわかる。尚、ＦＭＲにはＯＡＳＹＳがインストールされているが、ホスト計算機１１に登録されていないためＭＩＤは与えられていない。

【００３５】図７は、複数のユーザが１台の端末を共有する場合に、ホスト計算機１１が管理する情報の関係を示している。図７においては、ユーザＣ、Ｄ、Ｅの３人が１台の端末ＴＯＷＮＳを共有している。ユーザＣのユーザ情報は、ＵＩＤ＝０３、氏名Ｃ、キャッシュカードの情報、およびＬＯＴＵＳ－ＷＩＮの購入情報から成る。また、ユーザＤのユーザ情報は、ＵＩＤ＝０４、氏名Ｄ、キャッシュカードの情報、およびＦＭ秘書の購入情報から成る。また、ユーザＥのユーザ情報は、ＵＩＤ＝０５、氏名Ｅ、キャッシュカードの情報、およびＬＯＴＵＳの購入情報から成る。

【００３６】端末ＴＯＷＮＳのマシン情報は、ＭＩＤ＝３０、ソフト情報、機種Ｍ＝ＴＯＷＮＳ、およびＯＳ＝ＤＯＳ／ＴＯＳ／ＷＩＮから成る。ここで、ソフト情報は３人の共有者に販売したすべてのソフトウェアの名称、ＬＯＴＵＳ－ＷＩＮ、ＦＭ秘書、ＬＯＴＵＳを含んでいる。

【００３７】端末ＴＯＷＮＳのＭＩＤは、端末の登録時に共有者のうちの１人の代表者のＵＩＤと関係付けられる。ここでは、ＭＩＤ＝３０がユーザＣのＵＩＤと関係付けられている。この場合、ユーザＣはＭＩＤ＝３０の端末の問い合わせ先として３人の共有者を代表している。この例ではユーザＤがＦＭ秘書を購入しているが、ＦＭ秘書が破壊されたとき、ユーザＤ以外のどのユーザでもＭＩＤ＝３０を用いて復旧の要求を行い、無料で再インストール（復旧）のサービスを受けることができる。

【００３８】次に図８から図１１までを参照しながら、本実施例のソフトウェア流通システムにおける処理のフローを説明する。図８は、ユーザＩＤの登録処理のフローチャートである。図８において処理が開始されると、まずユーザは端末を流通センターのホスト計算機１１に接続して（ステップＳ１）、名前、キャッシュカードの番号、住所等の個人情報を入力する（ステップＳ２）。これを受けて、ホスト計算機１１は仮のユーザＩＤと仮のユーザパスワードを発行して、ユーザの仮登録を行う（ステップＳ３）。ここで、ユーザは一旦ホスト計算機１１との接続を断ち、キャッシュカードが認証されるのを待つ（ステップＳ４）。

【００３９】キャッシュカードが認証され、流通センターから正式のユーザＩＤと正式のユーザパスワードとが郵送されてくると（ステップＳ５）、ユーザは再び端末をホスト計算機１１に接続して（ステップＳ６）、受け取った正式のユーザＩＤと正式のユーザパスワードとを入力する（ステップＳ７）。これにより、ホスト計算機１１は正式のユーザＩＤとユーザパスワードを記載した郵便がユーザ本人に届いたことを確認し、そのユーザを正式に登録（本登録）して処理を終了する。このとき、郵送されたユーザパスワードと共に、別のパスワードをユーザが入力して登録することもできる。

【００４０】図９は、端末ＩＤの登録処理のフローチャートである。図９において処理が開始されると、まずユーザは端末を流通センターのホスト計算機１１に接続して（ステップＳ１１）、登録されているユーザＩＤとユーザパスワードを入力する（ステップＳ１２）。その後、端末がその機種や使用ＯＳ等のマシン情報を自動的にホスト計算機１１に送る（ステップＳ１３）。ホスト計算機１１は送られたマシン情報に端末ＩＤと端末パスワードを付加して所定の形式で記憶し、それらの端末ＩＤと端末パスワードを端末に送る（ステップＳ１４）。こうして、発行された端末ＩＤと端末パスワードは端末内にも保持される。

【００４１】図１０は、流通センターに登録されたユーザにネットワーク１２を介してソフトウェアを販売する処理のフローチャートである。図１０において、ユーザのリクエスト等により処理が開始されると、まずユーザの端末がネットワーク１２に接続される（ステップＳ２１）。次に、ホスト計算機１１はユーザが入力したユーザＩＤとユーザパスワードをチェックし（ステップＳ２２）、それらが正しくなければ（ＮＧ）、処理を終了する。

【００４２】ユーザＩＤとユーザパスワードが正しければ（ＯＫ）、次にホスト計算機１１は端末内に保持された端末ＩＤと端末パスワードとを自動的に読み取り、これらをチェックする（ステップＳ２３）。端末ＩＤと端末パスワードが正しくなければ（ＮＧ）、不正コピーが行われた可能性があるので不正に対応する処理（不正処理）を行う（ステップＳ２４）。

【００４３】端末ＩＤと端末パスワードが正しければ（ＯＫ）、商品であるソフトウェアのリストを端末の画面に表示させ、ユーザに購入する商品の選択を行わせる（ステップＳ２５）。ユーザは表示されたリストから商品を選択し、復旧サービスの要請の場合はその旨を入力する。

【００４４】次に、ホスト計算機１１はユーザからの要求が新規商品の購入か既に販売した商品の復旧要請かを判断し（ステップＳ２６）、復旧要請の場合はそのユーザの購入情報を参照して、該当する商品を過去に購入しているかどうかを調べる（ステップＳ２７）。ユーザが購入していない商品の復旧を要請している場合は（ステップＳ２７、ＮＯ）、復旧サービスの対象とならないので再びステップＳ２５の処理に戻る。

【００４５】ユーザが過去に購入した商品の復旧を要請している場合は（ステップＳ２７、ＹＥＳ）、ホスト計

算機１１はネットワーク１２を介してその商品を端末に宅配し、再インストールする　（ステップＳ２９）。そして、使用契約等に基づいてユーザに課金して（ステップＳ３０）、処理を終了する。ただし、無償で復旧サービスを行う契約が結ばれている場合は課金は行わない。

【００４６】ステップＳ２６でユーザが新規商品の購入を要求している場合は、選択された商品の販売を決定し（ステップＳ２８）、ネットワーク１２を介してその商品を端末に宅配してインストールする（ステップＳ２９）。そして、商品の代金をユーザに課金して（ステップＳ３０）、処理を終了する。

【００４７】ステップＳ３０においては、入力されたユーザＩＤを持つユーザに対して代金が課されるが、ユーザＩＤの管理はユーザに委ねられる。各ユーザはそのユーザパスワードを指定してユーザＩＤを管理する。商品の販売契約がユーザを対象とせずに、インストールする端末に対して販売することになっている場合は、ステップＳ３０において端末に対して代金が課金される。この場合は、ステップＳ２７においてその端末が該当する商品を過去に購入しているかどうかを調べ、購入していたときにのみ復旧サービスを行う。

【００４８】また、端末ＩＤについては、ホスト計算機１１が端末パスワードを付加し、端末が１回接続される毎にその端末の端末パスワードを自動的に書き換えて管理する。不正コピーが行われると、書き換え前の端末パスワードと共にアクセスが行われるため、その事実を認識することが可能になる。端末ＩＤおよび端末パスワードについては、ホスト計算機１１がバックトレースを行うことができる。

【００４９】図１１は、ステップＳ２３における端末パスワードのチェックと書換え、およびステップＳ２４の不正処理のフローチャートである。図１１において処理が開始されると、ホスト計算機１１は接続された端末の端末パスワードを、その端末の前回接続時に付与した端末パスワードと比較する（ステップＳ３１）。

【００５０】それらが一致すれば、新しい端末パスワードを生成してその端末内に書き込み、ホスト計算機１１内にも保持しておく（ステップＳ３２）。このとき、ホスト計算機１１は例えば乱数のように予想できないものを用いて、次の端末パスワードを決定する。また、書き換えられた古い端末パスワードは後で参照するために保存しておき（ステップＳ３３）、処理を終了する。

【００５１】ステップＳ３１で２つの端末パスワードが一致しないときは、ホスト計算機１１は不正コピーが行われたと判断し、接続された端末に新しい端末ＩＤを付与して新規に管理する（ステップＳ３４）。そして、接続時における端末パスワードを保存されている古い端末パスワードと順次比較して、その端末パスワードによるアクセスがあった日時を求める（ステップＳ３５）。これにより、不正コピーが行われたタイミングを特定して処理を終了する。

【００５２】図１２は、不正コピーが行われた場合の端末パスワードチェックの例を示している。図１２において、端末ＰＣＡのユーザがホスト計算機１１へのＮ回目のアクセスの後、使用しているソフトウェアと共にＭＩＤ＝１１とＭＰＳＷ＝１１１を、端末ＰＣＡのハードディスク（ＨＤ）から端末ＰＣＢのハードディスクに不正にコピーしたとする。このとき、ＰＣＡ、ＰＣＢ、ホスト計算機１１が保持するすべてのＭＩＤとＭＰＳＷが一致している。

【００５３】次に、Ｎ＋１回目のアクセスにおいてＰＣＡがアクセスを行う。ここでは、アクセスしたＰＣＡのＭＩＤとＭＰＳＷは、ホスト計算機１１が記憶しているＰＣＡのＭＩＤとＭＰＳＷと同じなので（ステップＳ３１）、不正コピーの事実は認識されない。そこで、ホスト計算機１１はＰＣＡのＭＰＳＷを２２２に書き換え、この新しいＭＰＳＷを保持する（ステップＳ３２）。

【００５４】次に、Ｎ＋２回目のアクセスにおいてＰＣＢがアクセスを行う。このとき、アクセスしたＰＣＢのＭＩＤはホスト計算機１１が記憶しているＰＣＡのＭＩＤと同じであるが、ＰＣ　ＢのＭＰＳＷはホスト計算機１１が記憶しているＰＣＡのＭＰＳＷと一致しない（ステップＳ３１）。ここで、ＰＣＢが前回にアクセスしたＰＣＡと異なる端末であることがわかり、不正コピーがあったことが認識される。

【００５５】そこで、ホスト計算機１１はＰＣＢのＭＩＤを１２に、ＭＰＳＷを３３３に書き換え、これらのＭＩＤとＭＰＳＷを保持する（ステップＳ３４）。こうして、ＰＣＢは新しい端末として登録され、新規に管理される。このような識別子の管理を行うことにより、悪意の無い不正コピーは防ぐことが可能である。しかし、悪意があってある程度の知識があれば、アクセス毎にＭＩＤとＭＰＳＷを端末間でコピーして使用することも可能である。このような場合には不正コピーを検出することは困難になる。そこで、ＭＩＤやＭＰＳＷを人為的にコピーするには手間がかかるようにしておく。例えば、隠しファイルの属性を持たせる方法や、これらを分散して配置する方法、端末の個別情報の組み合わせにより暗号化しておく方法等が考えられる。

【００５６】隠しファイルはＭＳＤＯＳ等で用いられるファイル属性の一つであり、ユーザは特別な操作をしないとその存在を知ることができないので、ここにＭＩＤやＭＰＳＷを書き込んでおけばコピーすることが困難になる。また、ＭＰＳＷの情報を分割して、端末のハードディスクの複数の箇所に分散して書き込んでおけば、それらの情報を探すのに手間がかかり、すべての情報が揃わなければＭＰＳＷを知ることはできない。

【００５７】また、端末のシリナルナンバー、ＦＯＲＭＡＴの日付、ファイルの物理位置等の機種別の情報や端末毎にバラツキのでる情報を用いて、所定の演算により

正しいＭＰＳＷが得られるようにしておいてもよい。所定の演算としては、乗算、除算、ＥＯＲ等の任意の演算の組合せを用いることができる。これにより、ＭＰＳＷを得る手続きが複雑になる。

【００５８】さらに、これらの方法を組み合わせて用いることも可能である。このようにしておけば、多大な手間をかけて多くのユーザが不正コピーを行うことは考えられなくなる。本発明の識別子管理装置により、コンピュータに対する知識が浅いために善意ではあるが契約に違反してしまう可能性のあるユーザの権利の保護と、ベンダーの保護とが共に図られることになる。また、悪意のあるユーザに対しては、例えばソフトウェアの不正コピーを行って使用するために多大な手間が要求される。

【００５９】上述した実施例によれば、ベンダーは不正コピーの事実があったかどうかと、不正コピーが行われたタイミングを認識することができるが、どういうルートでソフトウェアがコピーされたかを知ることは必ずしも可能ではない。そこで、販売するソフトウェア自体にマークを付加して、そのマークをホスト計算機１１に記憶しておく方法が考えられる。

【００６０】以下、図１３から図１９までを参照しながら、このマークを用いた識別子管理方法について説明する。ホスト計算機１１は、オンラインでソフトウェアを販売するときに、販売したソフトウェアを識別するマークとしてディストリビューションＩＤをそのソフトウェアに埋め込んでから送信する。このディストリビューションＩＤとしては、例えば販売先のユーザＩＤや端末ＩＤ、販売日時等の販売した事実を識別できる情報を用いる。特にディストリビューションＩＤとして購入したユーザのユーザＩＤを用いれば、ソフトウェアがコピーされた場合、それがだれに販売したものであるかを容易に知ることができる。

【００６１】図１３は、このときのマシン情報に含まれる販売記録の例を示している。図１３の販売記録は図５の販売記録にディストリビューションＩＤ（ＤＩＤ）が付加された形になっている。図１４は、ディストリビューションＩＤの設定処理のフローチャートである。図１４のディストリビューションＩＤの設定処理は、ソフトウェア作成者がソフトウェアを流通センターに登録するときに行われる。

【００６２】図１４において処理が開始されると、ホスト計算機１１はまずＤＩＤを埋め込む領域を、登録するソフトウェアのファイルの所定の位置に確保し（ステップＳ４１）、その領域の位置を記述したインストール用の定義ファイルを作成する（ステップＳ４２）。次に、そのソフトウェアと共に定義ファイルを登録して（ステップＳ４３）、処理を終了する。

【００６３】図１５は、ディストリビューションＩＤの埋め込み処理のフローチャートである。図１５のディストリビューションＩＤの埋め込み処理は、図１０のステップＳ２８で販売するソフトウェアが決定した後に行われる。図１５において処理が開始されると、ホスト計算機１１は販売するソフトウェアの定義ファイルを参照して、ディストリビューションＩＤを埋め込むファイルの名称とその中の埋め込み位置を特定する（ステップＳ４４）。次に、そのファイルの所定の位置に所定のディストリビューションＩＤを書き込んで（ステップＳ４５）、処理を終了する。

【００６４】図１６は、ディストリビューションＩＤのチェック処理のフローチャートである。図１６のディストリビューションＩＤのチェック処理は、ユーザが特定のソフトウェアを指定して、そのソフトウェアがコピーされたものかどうかをチェックするよう要請した場合に行われる。

【００６５】図１６において処理が開始されると、ホスト計算機１１はまず接続されたユーザの端末内に格納されているソフトウェアから、指定されたソフトウェアを検索する（ステップＳ５１、Ｓ５２）。指定されたソフトウェアがなければ処理を終了し、それがある場合は対応する定義ファイルを参照して、指定されたソフトウェアの所定の位置からディストリビューションＩＤを読み出す（ステップＳ５３）。次に、販売記録を参照して、読み出したディストリビューションＩＤが正しいかどうかを判定する（ステップＳ５４）。例えば、ディストリビューションＩＤとしてユーザＩＤを採用した場合は、ディストリビューションＩＤがアクセス時に入力されたユーザＩＤと一致していれば正しく、そうでなければ正しくない。

【００６６】ディストリビューションＩＤが正しければ、そのユーザのソフトウェアは不正にコピーされたものではないことを通知して（ステップＳ５５）、処理を終了する。また、ディストリビューションＩＤが正しくなければ、そのユーザのソフトウェアは何らかの形で不正にコピーされたものであることを通知して（ステップＳ５６）、処理を終了する。

【００６７】図１７は、ソフトウェアに埋め込まれたディストリビューションＩＤの例を示している。ここでは、例えばＷＩＮＤＯＷＳのＶＥＲＳＩＯＮＩＮＦＯリソースを用いて、ディストリビューションＩＤをファイル内に記録する。図１７において、ブロック”０４０９０４Ｅ４”内に記述された”ＡＡＡＡＡＡＡＡ”がディストリビューションＩＤの埋め込み領域に相当する。

【００６８】図１８は、このソフトウェアに対応するインストール用の定義ファイルの例を示している。図１８の定義ファイルには、ディストリビューションＩＤの埋め込み領域を設定したファイルの名称がＳＯＦＴ．ＥＸＥであり、そのアドレス８Ｅ８０から８文字が埋め込み領域であることが記述されている。

【００６９】登録されたソフトウェアの販売時には、ファイルを宅配する前に登録時のオリジナルファイル内の

13

ディストリビューションＩＤ埋め込み領域を、例えば販売先のユーザのユーザＩＤ等に書き換える。図１９は、図１７のディストリビューションＩＤの書き換えを示している。図１９において、ファイルＳＯＦＴ．ＥＸＥのアドレス８Ｅ８０から８Ｅ８７までに記述された”ＡＡＡＡＡＡＡＡ”の８文字が、宅配の前にディストリビューションＩＤ”ＧＤＦ０２２５６”に書き換えられる。

【００７０】こうして、販売されたソフトウェアのファイルにそのディストリビューションを識別できる情報が埋め込まれ、必要に応じてファイルからこの情報を読み出すことも可能になる。ディストリビューションＩＤはホスト計算機１１が設定するため、偽りの情報を使用することはできなくなる。また、ディストリビューションＩＤを埋め込んでいることをユーザに知らせることにより、ソフトウェアの不正コピーを抑制することができる。

【００７１】また、ディストリビューションＩＤにホスト計算機１１内だけに持っている情報を加えたり、暗号化技術を組み合わせたりすることにより、ユーザが勝手にディストリビューションＩＤを書き換えることは非常に困難になる。さらに、ソフトウェア作成者が、作成したソフトウェアの配布ルート等を調べる際にも利用できる。

【００７２】

【発明の効果】本発明によれば、オンラインでソフトウェアをインストール販売するシステムにおいて、ソフトウェアの販売履歴を効率的に管理し、ユーザとベンダーの双方にとって有益なサービスが可能となる。

【００７３】例えば、配布したソフトウェアが破壊された場合には、販売履歴を確認して、無償の復旧サービスが可能となる。これにより、ユーザはバックアップをとっておく手間が省けるし、ベンダーにとっては不正コピーを監視することができる。また、ユーザの要請に応じて、ソフトウェアがコピーされたものかどうかのチェックを行うこともできる。

【００７４】さらに、将来のソフトウェア流通システムにおいて、不正コピーを発見する機構が必要になったときに本発明を適用することもできる。

【図面の簡単な説明】

【図１】本発明の原理図である。

14

＊【図２】本発明の実施例のソフトウェア流通システムの構成図である。

【図３】ユーザ情報を示す図である。

【図４】マシン情報を示す図である。

【図５】販売記録を示す図（その１）である。

【図６】一人のユーザが複数の端末を持つ場合の情報を示す図である。

【図７】一台の端末を複数のユーザが共有する場合の情報を示す図である。

【図８】ユーザＩＤ登録のフローチャートである。

【図９】端末ＩＤ登録のフローチャートである。

【図１０】販売のフローチャートである。

【図１１】端末パスワードチェックのフローチャートである。

【図１２】端末パスワードのチェック例を示す図である。

【図１３】販売記録を示す図（その２）である。

【図１４】ディストリビューションＩＤの設定のフローチャートである。

【図１５】ディストリビューションＩＤの埋め込みのフローチャートである。

【図１６】ディストリビューションＩＤのチェックのフローチャートである。

【図１７】ディストリビューションＩＤの埋め込み領域の例を示す図である。

【図１８】定義ファイルの例を示す図である。

【図１９】ディストリビューションＩＤの書き換えを示す図である。

【符号の説明】

１管理手段
２端末パスワード変更手段
３ディストリビューション識別子付加手段
４ユーザ情報記憶手段
５端末情報記憶手段
６配布記録記憶手段
７定義ファイル格納手段
８ソフトウェア格納手段
１１ホスト計算機
１２ネットワーク
１３－１、１３－２、１３－ｍ端末

【図３】

ユーザ情報を示す図

UID . PSW . MID . ・・・ . 名前 . ・・・

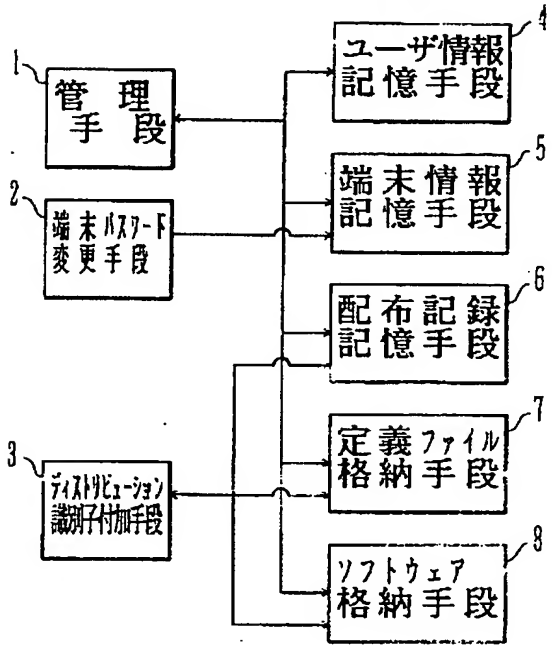
【図４】

マシン情報を示す図

MID . MPSW . UID . ・・・ . 機種	販売記録

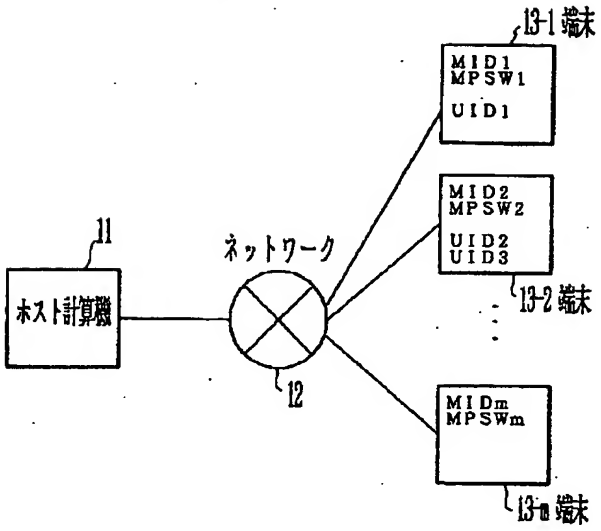
【図１】

本発明の原理図



【図２】

実施例の構成図



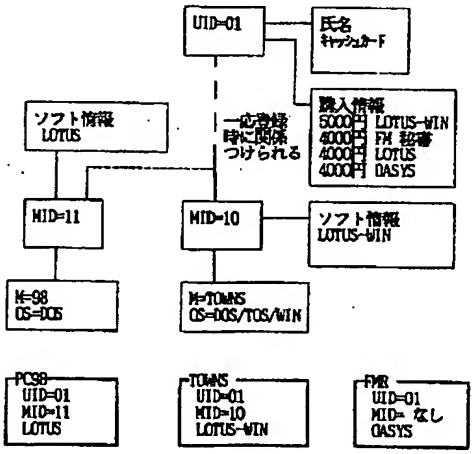
【図５】

販売記録を示す図（その１）

ソフトウェア名	ＵＩＤ	日　時

【図６】

一人のユーザが複数の端末を持つ場合の情報を示す図



【図１８】

定義ファイルの例を示す図

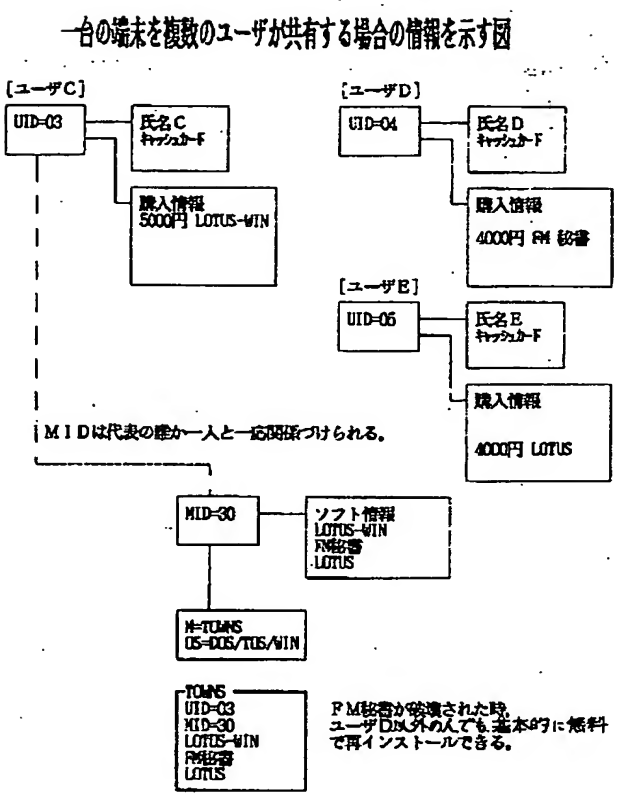
```
[MARK]
FILE=SOFT.EXE
index=8E80
NUM=8
```

【図１３】

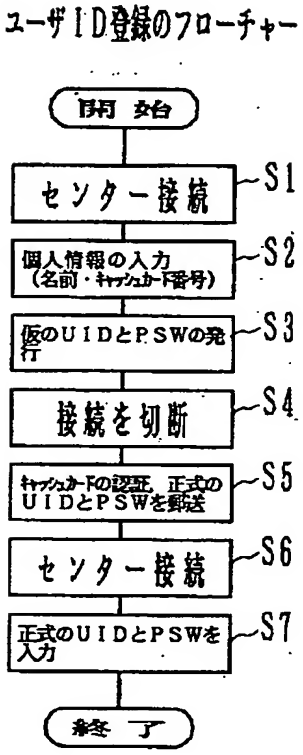
販売記録を示す図（その２）

ソフトウェア名	ＵＩＤ	日　時	ＤＩＤ

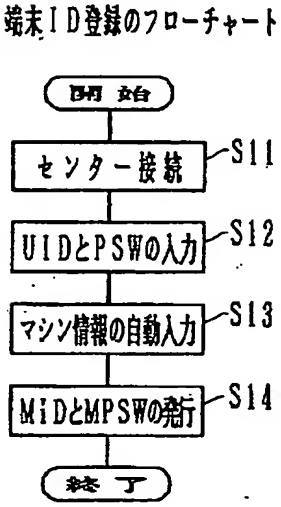
【図７】


一台の端末を複数のユーザが共有する場合の情報を示す図
[ユーザC]
UID=03
氏名C
キャッシュカードF
購入情報
5000円 LOTUS-WIN
[ユーザD]
UID=04
氏名D
キャッシュカードF
購入情報
4000円 FM 秘書
[ユーザE]
UID=05
氏名E
キャッシュカードF
購入情報
4000円 LOTUS
ＭＩＤは代表の誰か一人と一応関係づけられる。
MID=30
ソフト情報
LOTUS-WIN
FM秘書
LOTUS
M=TOWNS
05=005/TOS/WIN
TOWNS
UID=03
MID=30
LOTUS-WIN
FM秘書
LOTUS
ＦＭ秘書が破壊された時、
ユーザＩＤ以外の人でも基本的に無料
で再インストールできる。

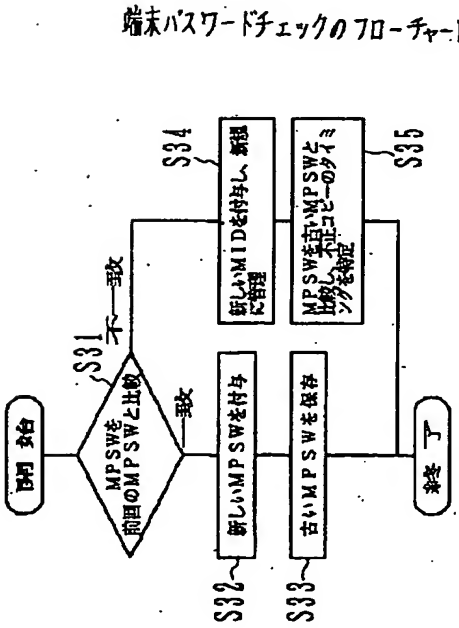
【図８】


ユーザＩＤ登録のフローチャート
開始
センター接続
S1
個人情報の入力
（名前・キャッシュカード番号）
S2
仮のＵＩＤとＰＳＷの発行
S3
接続を切断
S4
キャッシュカードの認証、正式のＵＩＤとＰＳＷを郵送
S5
センター接続
S6
正式のＵＩＤとＰＳＷを入力
S7
終了

【図９】

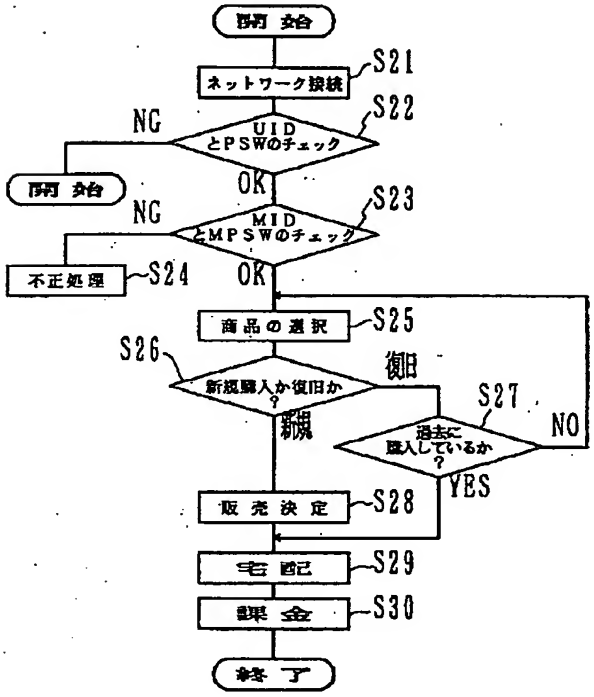

端末ＩＤ登録のフローチャート
開始
センター接続
S11
ＵＩＤとＰＳＷの入力
S12
マシン情報の自動入力
S13
ＭＩＤとＭＰＳＷの発行
S14
終了

【図１１】


端末パスワードチェックのフローチャート
開始
MPSWを前回のMPSWと比較
S31
不一致
一致
新しいMPSWを付与
S32
古いMPSWを保存
S33
新しいMIDを付与し、新規ＩＤ登録
S34
MPSWを古いMPSWとコピーのタイミングを確認
S35
終了

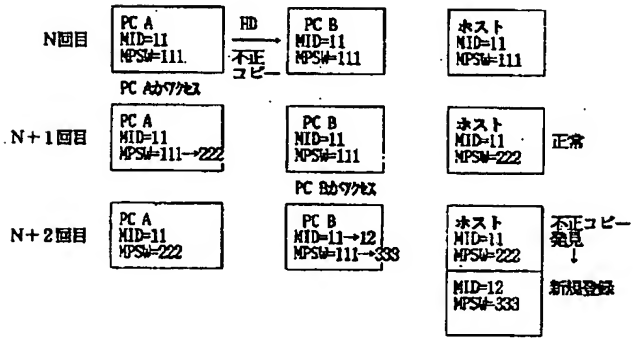
【図１０】

販売のフローチャート



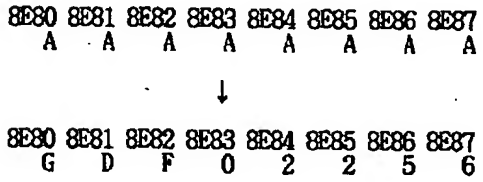
【図１２】

端末パスワードのチェック例を示す図



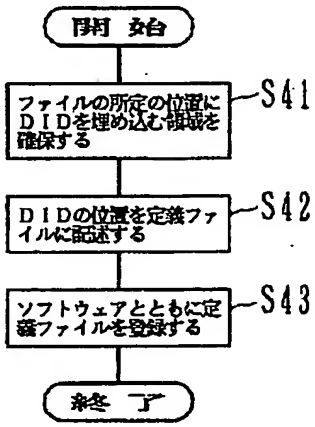
【図１９】

ディストリビューションＩＤの書き換えを示す図



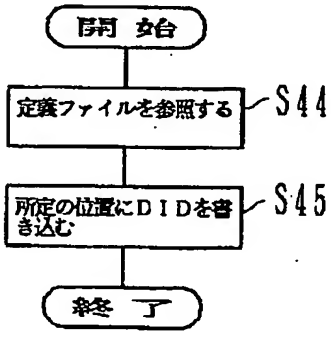
【図１４】

ディストリビューションＩＤの設定のフローチャート



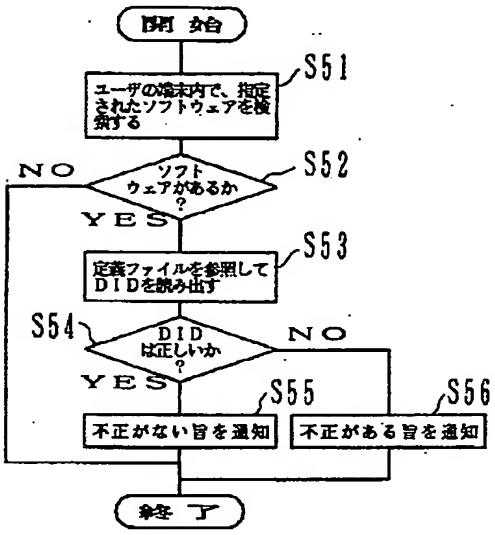
【図１５】

ディストリビューションＩＤの埋め込みのフローチャート



【図１６】

ディストリビューションＩＤのチェックのフローチャート



【図１７】

ディストリビューションＩＤの埋め込み領域の例を示す図

```
BLOCK "StringFileInfo"
BEGIN
    BLOCK "040904E4"
    BEGIN
        VALUE "Comment","AAAAAAAA"
        ～
    END
END
```

フロントページの続き

(72)発明者　沖　宏志
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　鎌田　紳二
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　原　孝
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　山嵜　利哉
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

Ｆターム(参考)　5B076 FC10